PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-181866
(43)Date of publication of application : 30.06.2000

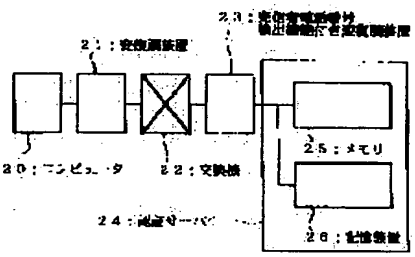
(51)Int.Cl. G06F 15/00
H04L 9/32
H04M 3/42
H04M 11/00

(21)Application number : 10-353597
(22)Date of filing : 11.12.1998

(71)Applicant : NEC SHIZUOKA LTD
(72)Inventor : OKURA HIROYUKI

(54) AUTHENTICATION SYSTEM

(57)Abstract:
PROBLEM TO BE SOLVED: To provide an authentication system which is safe even when a password is leaked.
SOLUTION: This authentication system, that is used when the connection of a caller's computer requested through a telephone line is performed, makes the user ID, password and called telephone number of a caller authentication information, comprises a modulating and demodulating device 23 with a caller telephone number detection function which has a caller's telephone number detection function, a memory 25 which temporarily stores a caller's telephone number notified from the device 23 and a user ID and a password transmitted by the caller and a storage device 26 which stores the authentication information of a user who is preliminarily allowed to connect and is provided with an authentication server 24 which collates stored contents of the memory 25 with caller's authentication information stored in the storage device 26.



LEGAL STATUS

[Date of request for examination] 11.12.1998
[Date of sending the examiner's decision of rejection]
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]
[Date of final disposal for application]
[Patent number]
[Date of registration]
[Number of appeal against examiner's decision of rejection]
[Date of requesting appeal against examiner's decision of rejection]
[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2000－181866
（P2000－181866A）
(43)公開日　平成12年６月30日(2000.6.30)

(51)Int.Cl.'	識別記号	ＦＩ		テーマコード'（参考）
Ｇ０６Ｆ　15/00	３３０	Ｇ０６Ｆ　15/00	３３０Ｂ	５Ｂ０８５
			３３０Ｃ	５Ｊ１０４
Ｈ０４Ｌ　9/32		Ｈ０４Ｍ　3/42	Ｔ	５Ｋ０２４
Ｈ０４Ｍ　3/42		11/00	３０３	５Ｋ１０１
11/00	３０３	Ｈ０４Ｌ　9/00	６７３Ａ	

審査請求　有　請求項の数４　ＯＬ　（全５頁）

(21)出願番号　特願平10－353597

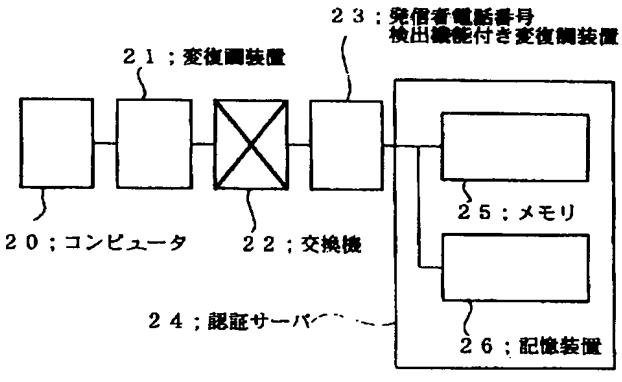
(22)出願日　平成10年12月11日(1998.12.11)

(71)出願人　000197366
静岡日本電気株式会社
静岡県掛川市下俣800番地
(72)発明者　大倉　宏之
静岡県掛川市下俣４番２　静岡日本電気株式会社内
(74)代理人　100108578
弁理士　高橋　昭男　（外３名）

最終頁に続く

(54)【発明の名称】　認証システム

(57)【要約】
【課題】　パスワードが漏洩した時でも安全な認証システムを提供する。
【解決手段】　電話回線を介して接続を要求された発信者のコンピュータを接続するときの認証システムであって、前記発信者のユーザーＩＤ、パスワードおよび発信電話番号を認証情報とすることを特徴とし、前記発信者の電話番号検出機能を有する発信者電話番号検出機能付き変復調装置と、この発信者電話番号検出機能付き変復調装置から通知された前記発信者の電話番号と前記発信者から送出されたユーザーＩＤおよびパスワードとを一時記憶するメモリと、予め接続を許可するユーザーの前記認証情報を記憶した記憶装置とからなり、前記メモリの記憶内容と前記記憶装置に記憶された前記発信者の認証情報との照合を行う認証サーバとを具備することを特徴とする。



【特許請求の範囲】
【請求項１】　電話回線を介して接続を要求された発信者のコンピュータを接続するときの認証システムであって、
前記発信者のユーザーＩＤ、パスワードおよび発信電話番号を認証情報とすることを特徴とする認証システム。
【請求項２】　前記発信者の電話番号検出機能を有する発信者電話番号検出機能付き変復調装置と、
この発信者電話番号検出機能付き変復調装置から通知された前記発信者の電話番号と前記発信者から送出されたユーザーＩＤおよびパスワードとを一時記憶するメモリと、予め接続を許可するユーザーの前記認証情報を記憶した記憶装置とからなり、前記メモリの記憶内容と前記記憶装置に記憶された前記発信者の認証情報との照合を行う認証サーバとを具備することを特徴とする請求項１に記載の認証システム。
【請求項３】　前記発信者の電話番号が検出されたとき、前記発信者のユーザーＩＤ、パスワードおよび発信電話番号を認証情報とし、
前記発信者の電話番号が検出されなかったとき、前記認証情報に接続回線が設定されていれば接続回線の電話番号が検出できないことを前記発信者に通知し、前記認証情報に接続回線が設定されていなければ前記発信者のユーザーＩＤおよびパスワードを認証情報とすることを特徴とする請求項１または２に記載の認証システム。
【請求項４】　電話回線を介して接続を要求された発信者の音声電話を接続するときの認証システムであって、
検出された電話番号が登録リストになかったときオペレーターが対応し、
検出された電話番号が登録リストにあったとき発信者に対してＩＤ番号の入力を促すことを特徴とする認証システム。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】この発明は、登録ユーザーの認証システムに関する。
【０００２】
【従来の技術】インターネットサービスプロバイダーによる登録ユーザーの認証は、ユーザーＩＤとパスワードによって行うのが一般的である。そのため、他人に悪用されないように、ユーザーは防衛手段としてパスワードのこまめな更新を行うのが一般的である。
【０００３】
【発明が解決しようとする課題】しかしながら、従来の認証システムにおいては、次のような課題があった。第１の課題は、認証がユーザーＩＤとパスワードで行われるため、他人の悪用防止策としてこまめなパスワードの更新が必要になり、煩わしかった。第２の課題は、認証がユーザーＩＤとパスワードのため、インターネットサービスプロバイダーのパスワードリストの漏洩や、ネットワーク上で盗み見されたりする可能性があり、パスワードを他人に悪用されるおそれがあるということである。このような場合、ユーザーは他人の悪用を防ぐ手段がなかった。
【０００４】本発明はこのような背景の下になされたもので、ユーザーＩＤとパスワード以外の認証条件に電話番号を加えることにより、パスワードの漏洩時でも安全な認証システムを提供することを目的とする。
【０００５】
【課題を解決するための手段】請求項１に記載の発明は、電話回線を介して接続を要求された発信者のコンピュータを接続するときの認証システムであって、前記発信者のユーザーＩＤ、パスワードおよび発信電話番号を認証情報とすることを特徴とする認証システムを提供する。
【０００６】請求項２に記載の発明は、前記発信者の電話番号検出機能を有する発信者電話番号検出機能付き変復調装置と、この発信者電話番号検出機能付き変復調装置から通知された前記発信者の電話番号と前記発信者から送出されたユーザーＩＤおよびパスワードとを一時記憶するメモリと、予め接続を許可するユーザーの前記認証情報を記憶した記憶装置とからなり、前記メモリの記憶内容と前記記憶装置に記憶された前記発信者の認証情報との照合を行う認証サーバとを具備することを特徴とする請求項１に記載の認証システムを提供する。
【０００７】また、請求項３に記載の発明は、前記発信者の電話番号が検出されたとき、前記発信者のユーザーＩＤ、パスワードおよび発信電話番号を認証情報とし、前記発信者の電話番号が検出されなかったとき、前記認証情報に接続回線が設定されていれば接続回線の電話番号が検出できないことを前記発信者に通知し、前記認証情報に接続回線が設定されていなければ前記発信者のユーザーＩＤおよびパスワードを認証情報とすることを特徴とする請求項１または２に記載の認証システムを提供する。
【０００８】さらに、請求項４に記載の発明は、電話回線を介して接続を要求された発信者の音声電話を接続するときの認証システムであって、検出された電話番号が登録リストになかったときオペレーターが対応し、検出された電話番号が登録リストにあったとき発信者に対してＩＤ番号の入力を促すことを特徴とする認証システムを提供する。
【０００９】
【発明の実施の形態】以下、この発明の一実施形態について図を参照しながら説明する。図１はこの発明による認証システムの概念を説明するためのブロック図である。図１において、符号１０は発信者電話番号検出機能付き変復調装置であり、発信者の電話番号を検出して検出結果をホストコンピュータ１１に送る。ホストコンピュータ１１はホストコンピュータ１１内にあるメモリ１

２に前記発信者の電話番号を保存する。電話回線接続後に発信者から送られてくるユーザーＩＤとパスワードも前記メモリ１２に保存する。

【００１０】ホストコンピュータ１１は、このホストコンピュータ１１内にユーザーＩＤ、パスワードおよび電話番号が記録されている記憶装置１３の情報とメモリ１２に保存されている前記発信者から送られてきた情報を照合して照合結果が同じだった場合に前記発信者を登録ユーザーと認証する。このようにして、本願発明では、認証をユーザーＩＤ、パスワードのほかに登録ユーザーの電話番号も使って行っているので、他人によるパスワードの悪用を防ぐことができる。

【００１１】次に、図２に本発明の一実施形態による認証システムの構成を示すブロック図を示す。この図において、発信者はコンピュータ２０をインターネットに接続するために、変復調装置２１を使ってダイヤルアップ接続をする。ダイヤル後、交換機２２は発信者電話番号検出機能付き変復調装置２３に発信者の電話番号を通知し、この発信者電話番号検出機能付き変復調装置２３は前記発信者の電話番号を検出して認証サーバ２４に電話番号を通知する。認証サーバ２４は内部にあるメモリ２５に電話番号を保存する。

【００１２】発信者電話番号検出機能付き変復調装置２３は電話番号を通知後、電話回線を接続して発信者から送られてくるユーザーＩＤ、パスワードを認証サーバ２４に通知する。認証サーバ２４はメモリ２５にユーザーＩＤ、パスワードを保存する。認証サーバ２４は認証サーバ２４の内部にある記憶装置２６からユーザーＩＤ、パスワード、登録されている電話番号の情報とメモリ２５内に保存している情報を照合して照合結果が同じだったとき、発信者を登録ユーザーであると認めてネットワークへの接続を許可する。

【００１３】次に図２の構成による本発明の一実施形態の動作を図３に示すフローチャートによって説明する。この図のステップＳ１（以下、Ｓ１等と略称する）において、発信者がインターネットサービスプロバイダーのアクセスポイントにダイヤルアップ接続すると、交換機２２はアクセスポイントの発信者番号検出機能付き変復調装置２３に電話情報（発信者の電話番号または発信者が電話番号を通知しない設定にしている場合はその設定情報）を通知する。発信者電話番号検出機能付き変復調装置２３は電話番号を検出し（Ｓ２）、認証サーバ２４に通知する。

【００１４】その後、発信者番号検出機能付き変復調装置２３は電話回線を接続して、発信者から送られてくるユーザーＩＤとパスワードを受信し（Ｓ３）、認証サーバ２４に通知する。認証サーバ２４は通知されてきた電話番号、ユーザーＩＤおよびパスワードを認証サーバ２４内のメモリ２５に保存し、さらに、この認証サーバ２４内の記憶装置２６に記録されている登録ユーザー情報（ユーザーＩＤ、パスワード、ユーザーが設定した発信先の電話番号）と前記メモリ２５に保存された情報とを照合する（Ｓ４）。

【００１５】この照合結果が同じだったとき、認証サーバ２４は発信者を登録ユーザーと認証してネットワークへの接続を許可する（Ｓ５）。もし、照合結果が同じでなかったとき、認証サーバ２４は認証情報が違うためネットワークに接続できないことを発信者に通知する（Ｓ６）。

【００１６】Ｓ２において、発信者電話番号検出機能付き変復調装置２３が電話番号を検出できなかった場合、発信者が電話番号を通知しない設定の場合は、その旨を認証サーバ２４に通知する。その後、発信者番号検出機能付き変復調装置２３は電話回線を接続して発信者から送られてくるユーザーＩＤとパスワードを受信し（Ｓ７）、認証サーバ２４に通知する。

【００１７】認証サーバ２４は通知されてきたユーザーＩＤ、パスワードを認証サーバ２４内のメモリ２５に保存し、通知されたユーザーＩＤのユーザーが発信する電話番号が設定されているかどうかを記憶装置２６の登録ユーザー情報と照合して確認する（Ｓ８）。ユーザーが発信する電話番号が登録されていた場合、認証サーバ２４は電話番号が検出できなかったため、ネットワークに接続できないことを発信者に通知する（Ｓ９）。

【００１８】認証サーバ２４はユーザーが発信する電話番号を設定していない場合、認証サーバ２４内にある登録ユーザー情報（ユーザーＩＤ、パスワード）とメモリ２５内の情報とを照合する（Ｓ１０）。この照合結果が同じだったとき、認証サーバ２４は発信者を登録ユーザーと認証してネットワークへの接続を許可する（Ｓ１１）。照合結果が同じでなかった場合は、認証サーバ２４は認証情報が異なるためネットワークに接続できないことを発信者に通知する（Ｓ１２）。

【００１９】上述のように、ダイヤルアップ接続するユーザーが契約時に発信する電話番号をインターネットサービスプロバイダーに連絡し、ダイヤルアップ接続時、インターネットサービスプロバイダーが発信者の電話番号を検出して、その電話番号を認証するための条件に加えることにより、パスワードが漏洩した場合、他人がダイヤルアップ接続しユーザーＩＤ、パスワードを使おうとしても、発信する電話番号が違う場合は認証されないので、他人の悪用を防げることを特徴としている。

【００２０】次に、図４に示す本発明の他の実施形態による認証システムの構成を示すブロック図について説明する。基本的構成は上述の一実施形態と同じであるが、通信販売等で発信者が電話機を使って通信した場合、受信システムに電話受信装置を使って発信者を認証している点についてさらに工夫している。

【００２１】図４において、発信者は電話機４０を使い、通信販売等の受付センターに電話をすると、交換機

４１は発信者の電話番号を発信者電話番号検出機能付き変復調装置４２に通知する。この発信者電話番号検出機能付き変復調装置４２は電話受信装置４３に発信者の電話番号を通知する。電話受信装置４３は電話受信装置４３内のメモリ４５に電話番号を保存し、電話受信装置４３内の記憶装置４４にある電話番号情報とメモリ４５の情報を照合する。

【００２２】照合の結果、電話受信装置４３は記憶装置４４にある電話番号情報の中にメモリ４５に保存している電話番号がなかったとき、オペレーターが受信するように電話回線を切り替える。電話受信装置４３は記憶装置４４にある電話番号情報の中にメモリ４５に保存している電話番号があったとき、発信者電話番号検出機能付き変復調装置４２に電話回線を接続させる。

【００２３】電話回線接続後、電話受信装置４３は発信者に事前に通知してあるＩＤ番号を押すよう発信者に通知し、発信者から通知されたＩＤをメモリ４５に保存し、記憶装置４４にある情報とメモリ４５に保存している情報を照合する。照合結果が同じだった場合、電話受信装置４３は発信者を登録ユーザーと認証して商品の注文等を受け付け、照合結果が異なる場合、電話受信装置４３はオペレーターに電話回線を転送する。このように、この実施形態では、電話受信装置４３を使って登録ユーザーを認証しているので、受付センターの人数の削減および登録ユーザーの電話受信装置４３による２４時間体制での受付ができるという効果が得られる。

【００２４】以上、本発明の２つの実施形態の動作を図面を参照して詳述してきたが、本発明はこの実施形態に限られるものではなく、本発明の要旨を逸脱しない範囲の設計変更等があっても本発明に含まれる。たとえば、使用する電話回線はアナログ回線と変復調装置の組み合わせでなく、ＩＳＤＮ回線であってもよい。

【００２５】

【発明の効果】これまでに説明したように、この発明による第１の効果は、認証に電話番号を使っているため、他人がパスワードを悪用しようとしても、発信する電話番号が違う場合、認証されないことである。

【００２６】第２の効果は、認証に電話番号を使っているため、登録している電話番号からダイヤルアップ接続する場合、パスワードのこまめな更新が必要なくなることである。

【００２７】第３の効果は、通信販売等で発信者が電話機を使って通信した場合、受信システムに電話受信装置を使って発信者を認証するようにしたので、通信販売等で受付センターの人数の削減および登録ユーザーの電話受信装置４３による２４時間体制での受付ができる。

【図面の簡単な説明】

【図１】　この発明による認証システムの概念を説明するためのブロック図である。

【図２】　この発明の一実施形態による認証システムの構成を示すブロック図である。

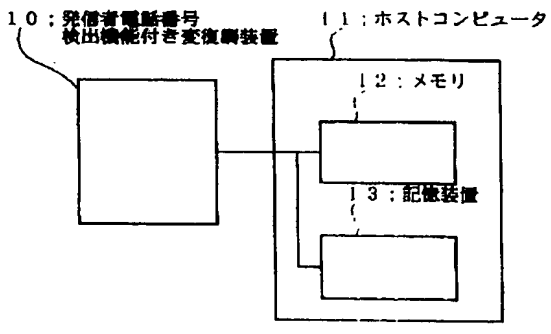
【図３】　この発明の一実施形態による認証システムの動作を示すフローチャートである。

【図４】　この発明の他の実施形態による認証システムの構成を示すブロック図である。

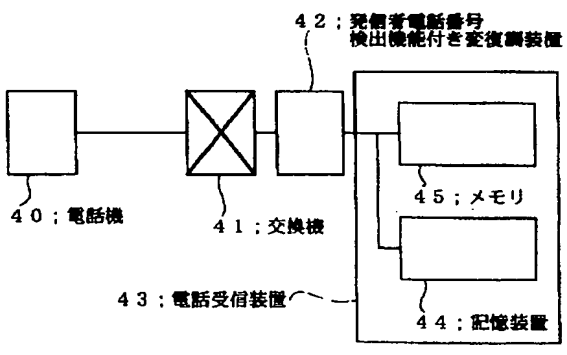
【符号の説明】

１０…発信者電話番号検出機能付き変復調装置
１１…ホストコンピュータ
１２…メモリ
１３…記憶装置
２０…コンピュータ
２１…変復調装置
２２…交換機
２３…発信者電話番号検出機能付き変復調装置
２４…認証サーバ
２５…メモリ
２６…記憶装置
４０…電話機
４１…交換機
４２…発信者電話番号検出機能付き変復調装置
４３…電話受信装置
４４…記憶装置
４５…メモリ

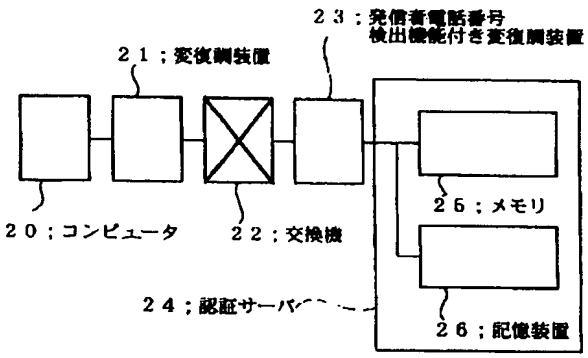
【図１】



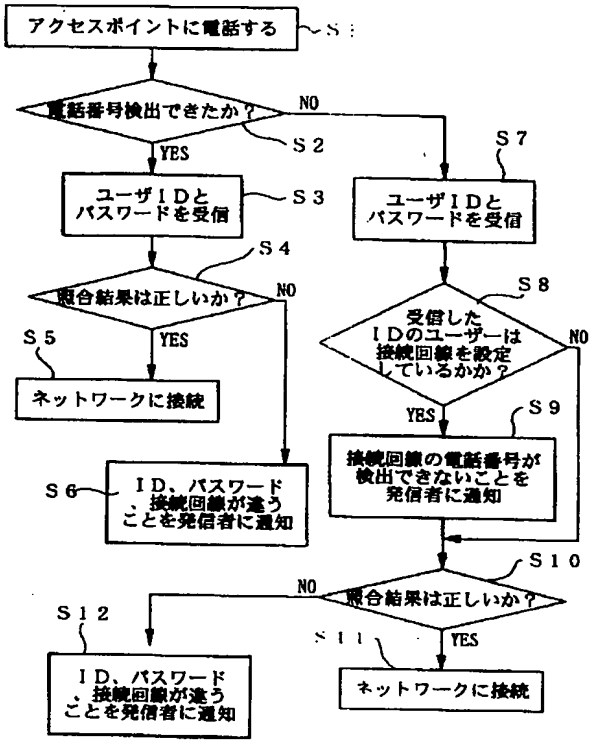
【図４】



【図２】



【図３】



フロントページの続き

Ｆターム(参考)　5B085 AE02 AE04 AE23
5J104 AA07 KA01 KA07 MA02 NA00
5K024 AA62 AA71 AA75 BB02 CC01
DD04 DD06 EE01 GG01 GG06
GG08 GG13
5K101 KK02 KK16 KK17 LL01 MM05
MM07 NN02 NN13 NN21 NN22
PP03 PP04 RR22 TT04 TT05
UU08